Planned Naval Staff Office Publication 5239 Modules (Note: the modules are not listed in publication order.)

Modules listed below with the **.exe** extension are available and are self extracable MS Word 6.0 documents. Estimated Isue Dated (EID) for Modules 07 and 08 are listed, below. The EID for the remaining documents will be posted as soon as they are available.

5239-01.exe   Introduction to Information Systems Security (INFOSEC)

Provides a basic introduction to INFOSEC and summaries the DoN INFOSEC Program.

5239-02.exe   Terms, Abbreviations, and Acronyms

Lists and defines INFOSEC terms, acronyms, and abbreviations that have been standardized for use within the DoN.

5239-03   Designated Approving Authority Guidebook

Provides guidance to the DAA in focusing the efforts of the activity security staff. Contains synopsis of certification and accreditation process. Offers the DAA a step-by-step approach to assist in reaching accreditation decisions.

5239-04.exe   Information Systems Security Manager Guidebook

Provides guidance to the individual assigned responsibility for INFOSEC implementation and operation at Navy activities. Additional TEMPEST guidance is provided for ISSMs at SYSCOMs, CINCs, and other echelon II commands. Illustrates the need for management involvement and support for the security program.

5239-07   Information Systems Security Officer's Guidebook
(Estimated Issue Date 01/31/96)
Aids those who carry out and administer INFOSEC programs for specific AISs and LANs. Helps ISSOs understand the requirements, identify the necessary planning, and conduct an effective INFOSEC program.

5239-08   Network Security Officer's Guidebook
(Estimated Issue Date 02/28/96)
Provides policy and step-by-step procedures to individuals responsible for accomplishing a risk analysis on WANs. Provides methods for the determination of system sensitivity and criticality, accomplishment of risk assessment and economic analysis, and determination of environmental hazards and threats to DoN information systems.

5239-10.exe   Assessed Product List

Identifies products which have been evaluated for features and assurance of trust.

5239-11   System Security Requirements Development

Provides guidance on how to develop a security policy and security requirements for a specific system.

5239-12   Acquisition Life Cycle Guidebook (PMs/Developers)

Identifies key technical and management actions need from Program Managers and other developers who have managerial and technical responsibilities for acquiring or certifying computer systems. Oriented primarily towards Program Managers, it focuses on the processes and requirements needed to certify and accredit information systems.

5239-13   Certification & Accreditation Guidebook

Provides procedural guidance and decision aids for conducting C&A process activities to determine the suitability of a system to operate in a targeted operational environment based on the degree of assurance required and other factors related to a system.

5239-14   Security Architecture Guidebook

Serves as a compendium of proven solutions to DON INFOSEC problems to assist INFOSEC systems engineering and customer support professionals to determine whether there are precedents for a customer's problem and to facilitate finding reusable solutions to common INFOSEC problems.

5239-15.exe   Controlled Access Protection Guide

Aids the user and security staff in understanding the DoN Controlled Access Protection policy, its relationship to C2, and techniques activities can use to acquire CAP compliant systems.

5239-16.exe   Risk Assessment Guidebook

Provides policy and step-by-step procedures to individuals responsible for accomplishing a risk analysis on systems. Provides methods for the determination of system sensitivity and criticality, accomplishment of risk assessment and economic analysis, and determination of environmental hazards and threats to DoN information systems.

5239-18   Security Test and Evaluation Guidebook

Provides information on how to perform security test and evaluation (ST&E) for information systems, embedded computers, and networks. It addresses microcomputers, minicomputers, mainframes, and specialized computers in both stand-alone and networked environments. The instruction provides general guidance and procedures to security managers and users for conducting ST&Es.

5239-19   Computer Incident Response Guidebook

Aids the, ISSM, ISSO, and users in responding to security incidents involving computer penetrations or malicious code. Provides general guidance for planning activity response and specific procedures for coordination with NAVCIRT.

5239-23   COMSEC Embedding Guidebook

Provides design guidelines for embedding INFOSEC modules.

5239-26.exe   Remanence Security Guidebook

Provides policy, guidelines, and procedures for clearing and purging information systems memory and other storage media for release outside of and for reuse within controlled environments. It pertains to both classified and sensitive unclassified information. Implements DOD 5200.28-M and CSC-STD-005-85.

5239-29.exe   Controls Over Copyrighted Computer Software

Assists DON activities in developing and implementing their own policies and procedures for controlling and using computer software programs having licensing agreements and copyright protection within the DON.